

Configuración del concentrador Cisco VPN 3000 en un router Cisco

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del concentrador VPN](#)

[Verificación](#)

[En el router](#)

[En el concentrador VPN](#)

[Troubleshooting](#)

[En el router](#)

[Problema - Incapaz de iniciar el túnel](#)

[PFS](#)

[Información Relacionada](#)

[Introducción](#)

Esta configuración de muestra muestra cómo conectar una red privada detrás de un router que funcione con el software del [®] del Cisco IOS a una red privada detrás del Cisco VPN 3000 Concentrator. Los dispositivos de las redes se reconocen entre sí por las direcciones privadas.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2611 Router con la versión de Cisco IOS Software 12.3.(1)**aNote:** Asegurese que los

Cisco 2600 Series Router están instalados con una imagen del IOS crypto del IPSec VPN que soporte la característica VPN.

- Cisco VPN 3000 Concentrator con 4.0.1 B

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

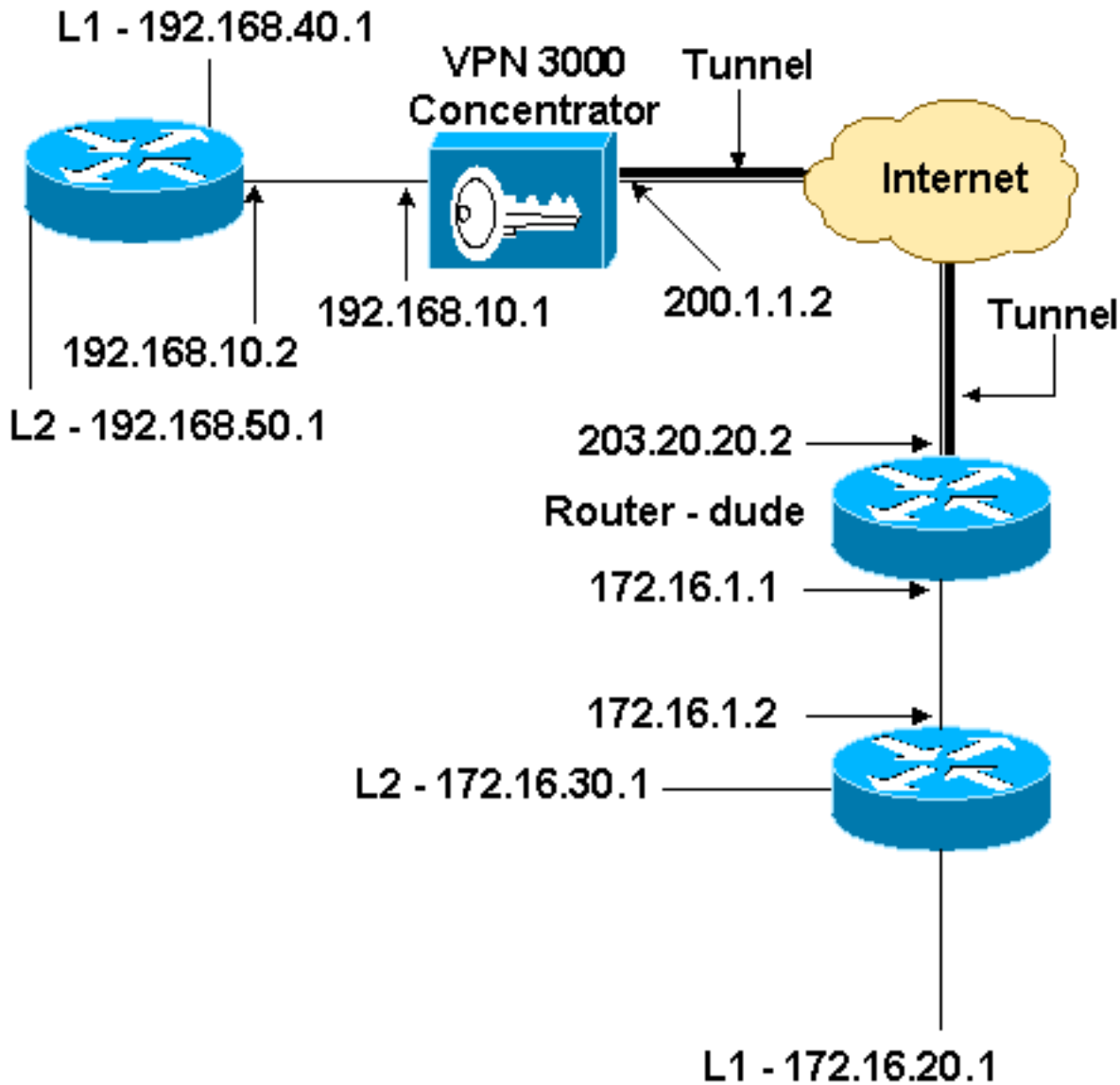
[Configurar](#)

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Use la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para encontrar más información sobre los comandos usados en este documento.

[Diagrama de la red](#)

Este documento utiliza esta configuración de red:



Configuraciones

Este documento utiliza esta configuración.

Configuración del router

```

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 200.1.1.2

```

```

!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
  set peer 200.1.1.2
  set transform-set to_vpn
!!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
  ip address 203.20.20.2 255.255.255.0
  ip nat outside
  half-duplex
  crypto map to_vpn
!
interface Ethernet0/1
  ip address 172.16.1.1 255.255.255.0
  ip nat inside
  half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!!--- Traffic to except from the NAT process. access-list
110 deny ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255

```

```
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

Configuración del concentrador VPN

En este entorno de laboratorio, el concentrador VPN primero se accede a través del puerto de la consola y se agrega una configuración mínima para poder hacer la configuración posterior con el Interfaz gráfica del usuario (GUI).

Elija el **Administration (Administración) > System reboot (Reinicio del sistema) > Schedule Reboot (Reinicio del programa) > Reboot with Factory/Default Configuration (Reinicio con configuración predeterminada/de fábrica)** para asegurarse de que no hay configuración existente en el concentrador VPN.

El concentrador VPN aparece en configuración rápida, y estos elementos se configuran después de la reinicialización:

- Fecha/hora
- Interfaces/Masks in Configuration > Interfaces (public=200.1.1.2/24, private=192.168.10.1/24)
- Gateway predeterminada en Configuration (Configuración) > System (Sistema) > ip routing (Ruteo de IP) > Default_Gateway (200.1.1.1) (Gateway predeterminada [200.1.1.1])

En este momento, el concentrador VPN es accesible con el HTML de la red interna.

Note: Porque el concentrador VPN se maneja de afuera, usted también tiene que seleccionar:

- **Configuration (Configuración) > Interfaces (Interfaces) > 2-public > filtro IP selecto > 1. soldados (valor por defecto).**
- **Administration (Administración) > Access Rights (Derechos de acceso) > Access Control List (Lista de control de acceso) > Add Manager Workstation** para agregar la dirección IP del *administrador externo*.

Esto no es necesario a menos que usted maneje el concentrador VPN del *exterior*.

1. Elija el **Configuration (Configuración) > Interfaces (Interfaces)** para volver a inspeccionar las interfaces después de que usted traiga para arriba el GUI.

Configuration | Interfaces Thursday, 03 July 2003 14:04:38
Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

• [Power Supplies](#)

2. Elija **Configuration > System > Routing IP >** los default gateways para configurar el gateway predeterminado (de Internet) y el gateway del valor por defecto del túnel (dentro) para que el IPSec alcance las otras subredes en la red privada.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Tunnel Default Gateway Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.

Override Default Gateway Check to allow learned default gateways to override the configured default gateway.

3. Elija **Configuration > Policy Management > Network Lists** crear las listas de red que definen el tráfico que se cifrará. Éstas son las redes locales:

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name Name of the Network List you are adding. The name must be unique.

Network List

192.168.10.0/0.0.0.255
 192.168.40.0/0.0.0.255
 192.168.50.0/0.0.0.255

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note:** Enter a *wildcard mask*, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Éstas son las redes remotas:

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Network List

```
172.16.1.0/0.0.0.255
172.16.20.0/0.0.0.255
172.16.30.0/0.0.0.255
```

Apply Cancel Generate Local List

4. Una vez terminado, estas son las dos listas de red: **Note:** Si no sube el túnel IPsec, marcar para ver si el tráfico interesante hace juego en los ambos lados. El tráfico interesante es definido por la lista de acceso en el router y los cuadros PIX. Son definidos por las listas de red en los concentradores VPN.

Configuration | Policy Management | Traffic Management | Network Lists

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List	Actions
VPN Client Local LAN (Default)	Add Modify Copy Delete
vpn_local_subnet	
router_subnet	

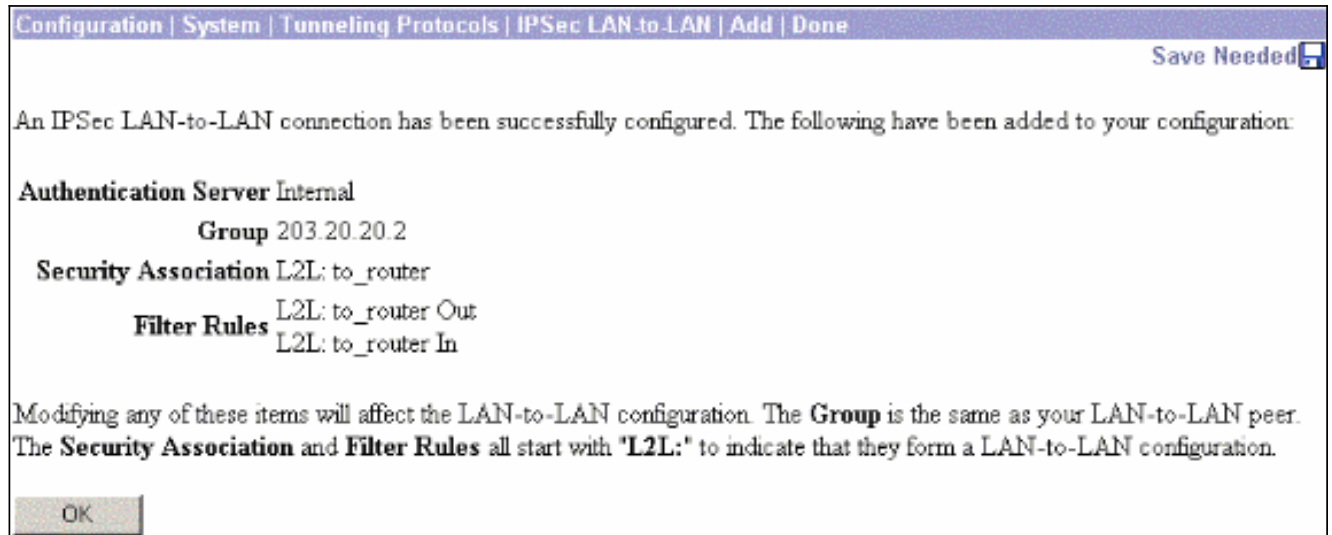
5. Elija el Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec LAN-to-LAN (IPSec de LAN a LAN) y defina el túnel de LAN a LAN.

Add a new IPSec LAN-to-LAN connection.

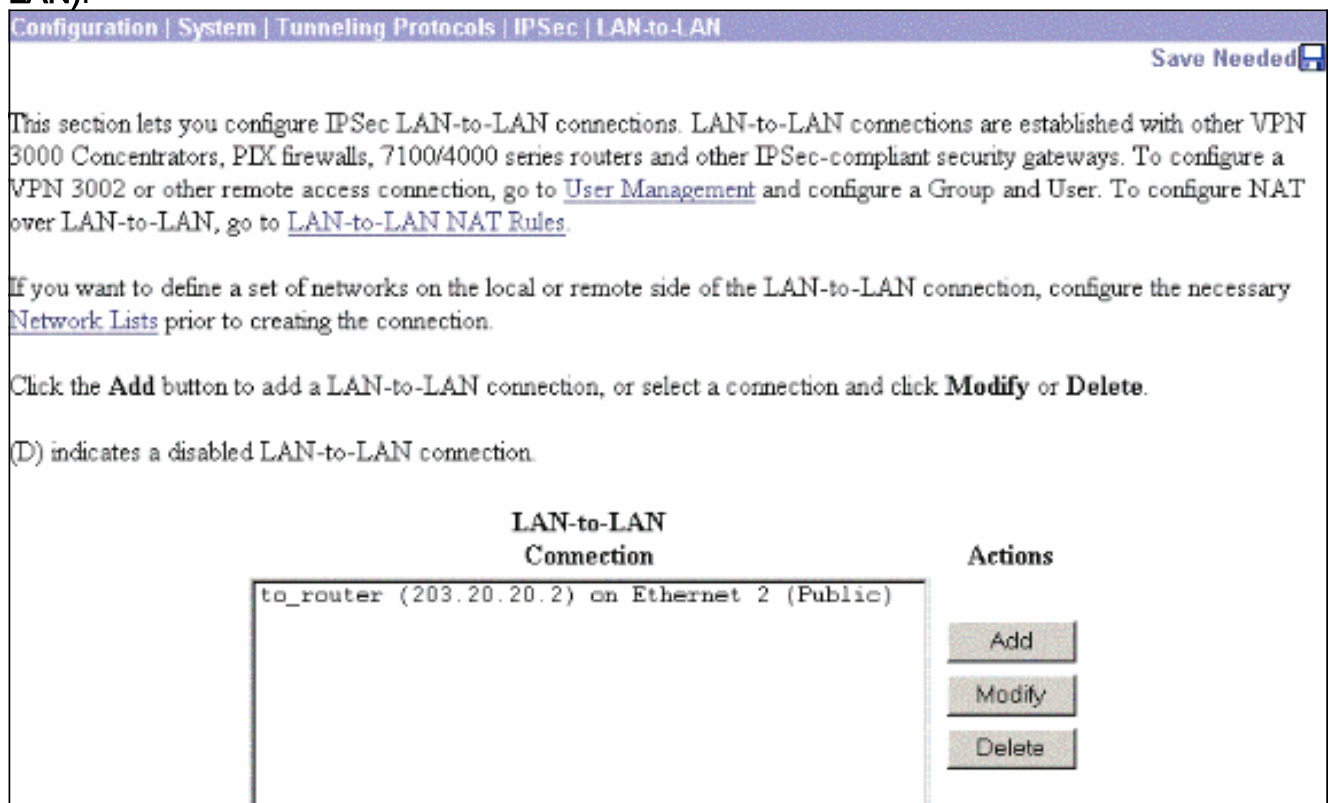
<p>Enable <input checked="" type="checkbox"/></p> <p>Name <input type="text" value="to_router"/></p> <p>Interface <input type="text" value="Ethernet2 (Public) (200.1.1.2)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid black; padding: 2px; min-height: 100px;"> <p>203.20.20.2</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate <input type="radio"/> Entire certificate chain</p> <p>Transmission <input checked="" type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text" value="cisco123"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p>
<p>Filter <input type="text" value="-None-"/></p> <p>IPSec NAT-T <input type="checkbox"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="None"/></p>	<p>Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.</p> <p>Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.</p>
<p>Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p>Network List <input type="text" value="vpn_local_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p>Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p>Network List <input type="text" value="router_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p>	

6. Después de que usted tecleo **se aplique**, esta ventana se visualiza con la otra configuración

que se crea automáticamente como resultado de la configuración del túnel de LAN a LAN.



Los parámetros de IPsec previamente creados del LAN a LAN se pueden ver o modificar en el Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPsec LAN-to-LAN (IPsec de LAN a LAN).



7. Elija el Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPsec > IKE Proposals (Propuestas IKE) para confirmar la oferta del IKE activo.

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.

Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient-3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7 IKE-3DES-MD5-RSA CiscoVPNClient-3DES-MD5-DH5 CiscoVPNClient-AES128-SHA IKE-AES128-SHA	<input type="button" value="« Activate"/> <input type="button" value="Deactivate »"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>	IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-RSA CiscoVPNClient-3DES-SHA-DSA CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA IKE-AES256-SHA

8. Elija el **Configuration (Configuración) > Policy Management (Administración de políticas) > Management Traffic (Administración de tráfico) > Security Associations (Asociaciones de seguridad)** para ver la lista de asociaciones de seguridad.

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPSec SAs	Actions
ESP-3DES-MD5 ESP-3DES-MD5-DH5 ESP-3DES-MD5-DH7 ESP-3DES-NONE ESP-AES128-SHA ESP-DES-MD5 ESP-L2TP-TRANSPORT ESP/IKE-3DES-MD5 L2L: to_router	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

9. Haga clic el Security Association name, y después haga clic **se modifican** para verificar las asociaciones de seguridad.

SA Name	<input type="text" value="L2L: to_router"/>	Specify the name of this Security Association (SA).
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="28800"/>	Specify the time lifetime in seconds.
IKE Parameters		
Connection Type	<input type="text" value="Bidirectional"/>	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
IKE Peers	<input type="text" value="203.20.20.2"/>	
Negotiation Mode	<input type="text" value="Main"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

Verificación

Esta sección enumera los **comandos show** usados en esta configuración.

En el router

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show crypto ipsec sa** - Muestra las configuraciones usadas por las asociaciones de seguridad actuales.
- **muestre isakmp crypto sa** — Muestra todas las asociaciones actuales de la seguridad de intercambio dominante de Internet en un par.
- **show crypto engine connection active** — Muestra las conexiones de sesión encriptada activas actuales para todos los motores de criptografía.

Usted puede utilizar la [herramienta de búsqueda de comandos del IOS \(clientes registrados solamente\)](#) para ver más información sobre los comandos determinados.

En el concentrador VPN

Elija el **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases) > Modify (Modificar)** para dar vuelta encendido a la registraci3n. Estas opciones est1n disponibles:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Gravedad de registro = 1-13

Gravedad en la consola = 1-3

Seleccione el **Monitoring (Monitoreo) > Event Log (Registro de evento)** para extraer el registro de acontecimientos.

Troubleshooting

En el router

Refiera a la [informaci3n importante en los comandos Debug](#) antes de que usted intente cualquier comando debug.

- debug crypto engine - Muestra el tr1fico cifrado.
- IPsec del debug crypto — Visualiza los IPsec Negotiations de la fase 2.
- isakmp del debug crypto — Visualiza negociaciones ISAKMP de la fase 1.

Problema - Incapaz de iniciar el t1nel

Mensaje de error

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
  set peer 200.1.1.2
```

```

set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
ip address 203.20.20.2 255.255.255.0
ip nat outside
half-duplex
crypto map to_vpn
!
interface Ethernet0/1
ip address 172.16.1.1 255.255.255.0
ip nat inside
half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask 255.255.255.0
ip nat inside source route-map nonat pool mypool overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!--- Traffic to encrypt. access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list 110 deny ip 172.16.1.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end

```

Solución

Complete esta acción para configurar el número deseado de logines simultáneos o fijar los logines simultáneos a 5 para este SA:

Van al Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos) > Modify 10.19.187.229 > los logines del general > de Simultaneouts y cambian el número de logines a 5.

En las negociaciones de IPsec, Perfect Forward Secrecy (PFS) garantiza que cada clave criptográfica nueva no esté relacionada a cualquier clave anterior. Habilite o inhabilite el PFS en ambos los peers de túnel. Si no, el túnel IPsec del LAN a LAN (L2L) no se establece en el Routers.

Para especificar que el IPsec debe pedir el PFS cuando solicitan las nuevas asociaciones de seguridad para esta entrada de correspondencia de criptografía, o que el IPsec requiere el PFS cuando recibe los pedidos las nuevas asociaciones de seguridad, utiliza el **comando set pfs** en el modo de configuración de la correspondencia de criptografía. Para especificar que el IPsec no debe pedir el PFS, no utilice la **ninguna** forma de este comando.

```
set pfs [group1 | group2]
no set pfs
```

Para el comando set pfs:

- *group1* — Especifica que el IPsec debe utilizar el grupo del módulo de la prima de Diffie Hellman del 768-bit cuando el nuevo intercambio Diffie-Hellman se realiza.
- *group2* — Especifica que el IPsec debe utilizar el grupo del módulo de la prima 1024-bit Diffie Hellman cuando el nuevo intercambio Diffie-Hellman se realiza.

De forma predeterminada, PFS no se solicita. Si no se especifica ningún grupo con este comando, como valor predeterminado se utiliza group1.

Ejemplo:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Refiera a la [referencia de comandos de la Seguridad de Cisco IOS](#) para más información sobre el comando set pfs.

Información Relacionada

- [Soluciones a los Problemas más frecuentes de IPsec VPN L2L y de Acceso Remoto](#)
- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3002 Hardware Clients](#)
- [Negociación IPsec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)